USPTO Scientific Technical Information Center

STIC EIC 2100 Search Request Form

119452

5U

Today's Date: 4/14/04

What date would you like to use to limit the search?

Priority Date: 8/27/99 Other:

Name Beemnet Dada

AU 2135 Examiner # 80215

Room # 6B08 Phone 703 305 8895

Serial # 09/645588

Format for Search Results (Circle One): PAPER DISK EMAIL

Where have you searched so far?

USP DWPI EPO JPO ACM IBM TDB IEEE INSPEC SPI Other web

Is this a "Fast & Focused" Search Request? (Circle One) YES NO

A "Fast & Focused" Search is completed in 2-3 hours (maximum). The search must be on a very specific topic and meet certain criteria. The criteria are posted in EIC2100 and on the EIC2100 NPL Web Page at http://ptoweb/patents/stic/stic-tc2100.htm.

What is the topic, novelty, motivation, utility, or other specific details defining the desired focus of this search? Please include the concepts, synonyms, keywords, acronyms, definitions, strategies, and anything else that helps to describe the topic. Please attach a copy of the abstract, background, brief summary, pertinent claims and any citations of relevant art you have found.

curve cryptography (elliptic, hyperelliptic) with Jacobian addition and Stickelberger element computing.

STIC Searcher Terese Esterheld Phone 308-7795

Date picked up 4/15/04 9:45am Date Completed 4/16/04 10:45am

sira Search and Information Resources Administration

```
Set      Items    Description
S1        7682    CURVE()CRYPTOGRAPH? OR ELLIPTIC OR HYPERELLIPTIC
S2         170    JACOBIAN
S3           0    STICKELBERGER
S4          11    S1 AND S2
File 347:JAPIO Nov 1976-2003/Dec(Updated 040402)
         (c) 2004 JPO & JAPIO
File 350:Derwent WPIX 1963-2004/UD,UM &UP=200423
         (c) 2004  Thomson Derwent
```

4/5/6 (Item 6 from file: 347)
DIALOG(R)File 347:JAPIO

06839492 **Image available**
SECURE PARAMETER GENERATING DEVICE AND METHOD FOR ALGEBLAIC **CURVE CRYPTOGRAPH**, AND RECORDING MEDIUM

PUB. NO.: 2001-066987 [JP 2001066987 A]
PUBLISHED: March 16, 2001 (20010316)
INVENTOR(s): ARITA MASATAKE
APPLICANT(s): NEC CORP
APPL. NO.: 11-242075 [JP 99242075]
FILED: August 27, 1999 (19990827)
INTL CLASS: G09C-001/00

ABSTRACT
PROBLEM TO BE SOLVED: To improve the security of an algebraic **curve cryptograph** by enabling a complicated high order algebraic curve, which can not conventionally be used, for the algebraic **curve cryptograph**.

SOLUTION: A Stickerberger element calculating unit 11 calculates a Stickerberger element (ω) in a, b divided fields of a circle, then an Jacobi sum candidate value calculating unit 12 calculates an Jacobi sum cadidate value (j) and a prime number (p) corresponding to the Jacobi sum candidate value (j) from a prime number (a), a prime number (b), the size (n) of a cryptographic key and the Stickerberger element (ω) and an order candidate value calculating unit 13 calculates a set H consisting of plural candidates of the order of the **Jacobian** group of an algebraic curve from the prime number (a), the prime number (b) and the Jacobi sum cadidate value (j) and a safety judging unit 14 retrieves a candidate value (h) satisfying a safety condition of an almost prime property or the like from among the set H and a parameter deciding unit 15 calculates parameters of an algebraic curve which is specified by the prime number (a), the prime number (b) and the prime number (p) and whose order of the **Jacobian** group coincides with the candidate value (h).

4/5/7 (Item 7 from file: 347)
DIALOG(R)File 347:JAPIO

06595550 **Image available**
METHOD FOR COMPUTING POINT ON **ELLIPTIC** CURVE ON ELEMENT ASSEMBLY AND APPARATUS THEREFOR

PUB. NO.: 2000-181347 [JP 2000181347 A]
PUBLISHED: June 30, 2000 (20000630)
INVENTOR(s): ITO KOICHI
TAKENAKA MASAHIKO
TORII NAOYA
TENMA SHOJI
KURIHARA YASUSHI
APPLICANT(s): FUJITSU LTD
APPL. NO.: 10-361491 [JP 98361491]
FILED: December 18, 1998 (19981218)
INTL CLASS: G09C-001/00; G06F-007/72

ABSTRACT
PROBLEM TO BE SOLVED: To enable addition processing without executing inverse number computation and to enable high-speed processing without adding additive coordinates by using the **Jacobian** coordinates obtained by three-dimensionally projecting the points on an **elliptic** curve on an element assembly.

SOLUTION: In the method of executing the computation by combining the double calculation processing and addition processing in accordance with the multiplier converted to a binary digit system expressed, the points (x, y) on the **elliptic** curve on the element assembly are converted to the **Jacobian** coordinate expression of attaining (x, y)=(X/Z2, Y/Z3) and in the case of continuous execution of the double calculation processing, the computation results (Xt+1, Yt+1, Zt+1) at the point of the time (t+1) of the continuous double calculation processing is subjected to the arithmetic processing with the calculation equation shown by the equation using the present **Jacobian** coordinates (Xt, Yt, Zt). In such a case, the value of Y' which is the value of twice the Y coordinate is first calculated and the number of times of the addition system in the double calculation at the point of the **Jacobian** coordinates is decreased by using the value of Y'.

4/5/8 (Item 8 from file: 347)
DIALOG(R)File 347:JAPIO

06551707 **Image available**
CALCULATING METHOD OF POINT ON **ELLIPTIC** CURVE ON PRIME FIELD AND DEVICE THEREFOR

PUB. NO.: 2000-137436 [JP 2000137436 A]
PUBLISHED: May 16, 2000 (20000516)
INVENTOR(s): TAKENAKA MASAHIKO
ITO KOICHI
TORII NAOYA
APPLICANT(s): FUJITSU LTD
APPL. NO.: 10-311379 [JP 98311379]
FILED: October 30, 1998 (19981030)
INTL CLASS: G09C-001/00

ABSTRACT

PROBLEM TO BE SOLVED: To enable addition processing without performing reciprocal operation and to enable high speed processing without involving an additional coordinates by using **Jacobian** coordinates obtained by projecting a point on an **elliptic** curve on a prime field is projected in the three dimensional space.
SOLUTION: When points (x, y) on an ellipse curve on a prime field indicated by y2=x3+ax+b(mod p) is multiplied by a multiplier, this is a method in which doubling calculation processing and addition processing are combiningly performed based on the multiplier converted into binary number system expression. And the points (x, y) is converted to **Jacobian** coordinates being (x, y)=(X/Z2, Y/Z3), when doubling calculation processing is continuously performed, calculation processing in which a calculated result at the point of time (t+1) of continued doubling calculation processing is indicated in an equation using the present **Jacobian** coordinates. Then, in calculation processing at the point of time (t+1), doubling calculation processing is performed using a Zt-14 and 8Yt-14 used when a calculation result at the point of time (t) of previous stage is obtained, while obtained a Zt4 and 8Yt4 are stored.

4/5/9 (Item 9 from file: 347)
DIALOG(R)File 347:JAPIO

06340744 **Image available**
HYPERELLIPTIC CURVE ENCIPHERING METHOD, AND ITS DECORDING

PUB. NO.: 11-282348 [JP 11282348 A]
PUBLISHED: October 15, 1999 (19991015)

INVENTOR(s): WATANABE KAZUO
APPLICANT(s): SONY CORP
APPL. NO.: 10-086603 [JP 9886603]
FILED: March 31, 1998 (19980331)
INTL CLASS: G09C-001/00

ABSTRACT

PROBLEM TO BE SOLVED: To shorten cipher processing time.

SOLUTION: Elements of a **Jacobian** variety are utilized as several kinds of pairs of points on a **hyperelliptic** curve for a disclosure key used in the case of enciphering an ordinary sentence in a **hyperelliptic** curve enciphering method using the **Jacobian** variety accompanied to the **hyperelliptic** curve, and for an operation of addition on the **Jacobian** variety used in the case of decording encipherment using the disclosure key. However, pairs of points replaced by a point at infinity are used if necessary not to come into a conjugated relation each other among the points which are not points at infinity out of the points on the **hyperelliptic** curve. Conjugated relations of the points constituting the elements and number of point at infinity thereof are marked to reduce calculation in the case of addition operation on the **Jacobian** variety. A cipher processing time is shortened thereby in the present invention compared with conventional one while securing difficulty for a discrete logarithm problem.

4/5/10 (Item 10 from file: 347)
DIALOG(R)File 347:JAPIO

06270870 **Image available**
ELLIPTIC CURVE OPERATION DEVICE

PUB. NO.: 11-212458 [JP 11212458 A]
PUBLISHED: August 06, 1999 (19990806)
INVENTOR(s): MIYAJI MITSUKO
ONO TAKATOSHI
APPLICANT(s): MATSUSHITA ELECTRIC IND CO LTD
APPL. NO.: 10-013748 [JP 9813748]
FILED: January 27, 1998 (19980127)
INTL CLASS: G09C-001/00; G09C-001/00; G09C-001/00; H04L-009/30

ABSTRACT

PROBLEM TO BE SOLVED: To provide an **elliptic** curve operation device in a quick cipher and signature system.

SOLUTION: In an auxiliary calculation table generation step 1, an auxiliary calculation table is generated with affine coordinates. In a kP calculation step 2, kP is obtained by mixture coordinates where addition to values (affine coordinates) of the auxiliary calculation table is obtained in revised **Jacobian** coordinates and the result is multiplied by power of two in correction **Jacobian** coordinates but the final result is obtained in **Jacobian** coordinates. Mixture coordinates and revised **Jacobian** coordinates are used to reduce the number of multiplications.